BIB Designの不存在証明について (デザインの構成法および不存在性)

数理解析研究所講究録
285巻 1976年 88-95

BIB designの不存在証明について

創価大 経済 池田貞雄
カルガリ大 小川潤次郎

序 対称BIBD($v=b$, $r=k$, λ)の場合には、その結合行列Nは正方行列で、$NN' \sim I_v$(有理合同:$\sim$)に対して Hasseの定理を適用した判定条件

$$|NN'| \sim 1, \quad C_p(NN') = +1 \text{（すべての素数 } p \text{ で）}$$

が得られているが、この条件はかなり強いものであろうと思われている。

非対称な場合には、しかし、対称な場合に類した判定条件を導くことは、少くとも Hasseの定理を用いようとする立場からは非常に困難である。筆者らは、これまで多くのいろいろな方法で試みたが、すべて identity に終り、未だ結果的には何も得られていない。

この報告では、これまで試みてきた方法のうちで、代表的なものいくつかを紹介して、前車の轍としたい。また、$\lambda=1$の場合には、ブロック・アソシエーションを利用した不存在証

明の方向があることを述べたい。

1. 結合行列を用いる方法 (I)

BIBD(v,k,b,r,λ) の結合行列 $N_{v\times b}$ を用いて

$$(1.1)\qquad P=\begin{bmatrix} N & \rho I_v \\ I_b & N' \end{bmatrix}_{\overline{v+b}\times\overline{v+b}} .$$

を作ると，

$$PP'=\begin{bmatrix} NN'+\rho^2 I_v & (1+\rho)N \\ (1+\rho)N' & I_b+N'N \end{bmatrix}$$

となり，$\rho=(r-\lambda-1)/2$ のときこれは

$$(1.2)\qquad PP'\sim\begin{bmatrix} (r-\lambda+\rho^2)I_v+\lambda G_v & 0 \\ 0 & I_b+\dfrac{\lambda k^2}{rk+\rho^2}G_b \end{bmatrix} .$$

$PP'\sim I_{v+b}$ に Hasse の定理を用いて

$$(1.3)\qquad \begin{cases} (rk+\rho^2)\left(1+\dfrac{\lambda k^2 b}{rk+\rho^2}\right)\sim 1 \\ \left(rk+\rho^2,\ 1+\dfrac{\lambda k^2 b}{rk+\rho^2}\right)_p(-1,\ rk+\rho^2)_p(v,\ rk+\rho^2)_p\left(-1,\ 1+\dfrac{\lambda k^2 b}{rk+\rho^2}\right)_p \\ \qquad\left(v,\ 1+\dfrac{\lambda k^2 b}{rk+\rho^2}\right)_p=+1 \end{cases}$$

が得られるが，これらは $vr=bk,\ \lambda(v-1)=r(k-1)$ の下で恒等的に成立する．

この方法の変型として，各種のものが考えられる。たとえば，(1.1) の N' の所を $G_{b,v}$ におきかえたらどうなるか，ある

は，Nの替りにいくつかの rows を落した行列を用いたら？，Pの第1行を落して $\overline{v+b-1}\times\overline{v+b}$ 行列に Hasse theorem の Hasse-Minkowski の p-invariant に関する条件を適用したらどうなるか，等々である。しかし，これらはすべて identity になる。

2. 結合行列を用いる方法 (II)

N の row-space (rational field 上の) の直交補空間の中から $b-v$ 個の線形独立な rational vectors を選び，それらを行とする $\overline{b-v}\times b$ 整行列を S とする。

$$(2.1)\qquad P=\begin{bmatrix} N \\ S \end{bmatrix}$$

とおくと，

$$(2.2)\qquad PP'=\begin{bmatrix} NN' & 0 \\ 0 & Q \end{bmatrix},\quad Q=SS'.$$

したがって，

$$(2.3)\qquad \begin{cases} |Q|=|NN'|=(r-\lambda)^{v-1}rk, \\ C_p(Q)=(-1,-1)_p(-1,|NN'|)_p\,C_p(NN'). \end{cases}$$

(2.1) の N のところに，たとえば つぎの $\overline{v-1}\times b$ 行列

$$M=\begin{bmatrix} J_b' \\ N_2 \end{bmatrix},\quad (N_2 \text{ は } N \text{ の第}3\sim v\text{行の submatrix})$$

を入れて

$$(2.4)\qquad P=\begin{bmatrix} M \\ S \end{bmatrix}$$

に対して条件

$$(2.5) \qquad c_p(PP') = \cancel{+1}(-1,-1)_p$$

を調べてみる.

$$MM' = \begin{bmatrix} b & rJ'_{v-2} \\ rJ_{v-2} & (r-\lambda)I_{v-2}+\lambda G_{v-2} \end{bmatrix} \sim \begin{bmatrix} b & 0 \\ 0 & (r-\lambda)I_{v-2}+(\lambda-\frac{r^2}{b})G_{v-2} \end{bmatrix},$$

$$PP' = \begin{bmatrix} MM' & 0 \\ 0 & Q \end{bmatrix}$$

より, (2.5) は, $g \equiv r-\lambda+(v-2)(\lambda-\frac{r^2}{b})$ とおいて

$$(b,(r-\lambda)^{v-3}g)_p\,(b,|Q|)_p\,((r-\lambda)^{v-3}g,|Q|)_p\,(-1,b)_p\,c_p((r-\lambda)I_{v-2}+(\lambda-\tfrac{r^2}{b})G_{v-2})\cdot c_p(Q)$$

$$\equiv (b,(r-\lambda)^{v-1}g)_p\,(b,(r-\lambda)^{v-1}rk)_p\,((r-\lambda)^{v-1}g,(r-\lambda)^{v-1}rk)_p\,(-1,b)_p$$

$$(2.6) \qquad (-1,r-\lambda)_p^{\frac{(v-2)(v-3)}{2}}(-1,g)_p\,(v-2,g)_p\,(v-2,r-\lambda)_p\,(g,r-\lambda)_p^{v-3}\,(-1,(r-\lambda)^{v-1}rk)_p$$

$$(-1,r-\lambda)_p^{\frac{v(v-1)}{2}}(-1,rk)_p\,(v,rk)_p\,(v,r-\lambda)_p\,(rk,r-\lambda)_p^{v-1} \qquad = +1$$

となる。これは identity であることが示される.

この方法についてもいろいろな変型が考えられる. たとえば, (2.1) の N の右かたに, もう1列, $\begin{bmatrix} J_m \\ 0 \end{bmatrix}$ の形の列を加え

$$P = \begin{bmatrix} J_m & N \\ 0 & \\ 0 & S \end{bmatrix}$$

に $c_p(PP') = +1$ を適用することもできるし,

$$P = \begin{bmatrix} 1 & a \\ J_m & N \\ 0 & \\ 0 & S \end{bmatrix}, \quad \left(\begin{array}{l} a \text{ は } N \text{ の row-space の中の vector で} \\ N \text{ との関係がわかっているもの} \end{array} \right)$$

の形のものを考えることもできる。しかし, これらもすべて

identity になる。

3. $\lambda=1$ の場合 (I)

この場合には、上述(I), (II) で扱った方法以外に、ブロックの association を利用する方法も考えられる。まず

$$(3.1)\qquad \begin{cases} NN' = (r-1)\, I_v + G_v \\ N'N = k\, I_b + A_1 = rk\, A_0^{\#} + (r-1)\, A_1^{\#}. \end{cases}$$

N の row space の orth.-compl. は $A_2^{\#}$ の中の vector の張る space で、実際 $A_2^{\#}$ の row (or column) space になっている。したがって、(2.1) の S の部分には、その space の basis vector をもってくればよい。前節 (II) の方法と同じように、(2.1) の N のいくつかの rows を $A_1^{\#}$ の中の vectors でおき替えることを考えてみる。

(3.1) から

$$(3.2)\qquad N A_1^{\#} = N - \frac{r}{b} G_{v,b}$$

N の最後の $v-m$ rows からできる submatrix を N_m, $A_1^{\#}$ の（最初の 又は任意の）m 個の rows のつくる $m\times b$ 行列を C_m として

$$(3.3)\qquad P = \begin{bmatrix} N_m \\ C_m \\ S \end{bmatrix}$$

を考えると、

$$(3.4)\qquad PP' = \begin{bmatrix} N_m N_m' & N_m C_m' & 0 \\ C_m N_m' & C_m C_m' & 0 \\ 0 & 0 & Q \end{bmatrix}.$$

ここで、C_mC_m' の部分は、ブロック関係のはっきりしている、たとえば、互に 1-st associates (SLBで) な r 個のブロックに対応する $A_1^{\#}$ の rows の中から C_m を選べば、計算可能。また N_mC_m' の部分は、適当なブロックと処理の配列をとれば (3.4) からわかる。

詳細は省略するが、$m=1$ の場合に $A_1^{\#}$ の第1列を C_m としてとると、$d_1=\eta_0-\frac{\eta_{11}}{r-1}+\frac{\gamma_{11}}{(r-1)(rk-1)}$, $\eta_{11}=\alpha^2(k-1)+\beta^2(v-k)$, $\gamma_{11}=(\alpha(k-1)-\beta(v-k))^2$, $\eta_0=\frac{k(k-1)}{v}$, $\alpha=1-\beta$, $\beta=\frac{k}{v}$ として

$$
(3.5)\quad\left\{\begin{array}{l}
d_1\cdot rk(rk-1)(r-1)\sim 1,\\
(d_1,(r-1)^{v-2}(rk-1))_p(-1,d_1)_p(-1,r-1)_p^{\frac{v(v-1)}{2}}(-1,rk)_p(v,rk)_p(v,r-1)_p\\
(rk,r-1)_p^{v-1}(-1,r-1)_p^{\frac{(v-1)(v-2)}{2}}(-1,rk-1)_p(v-1,rk-1)_p(v-1,r-1)_p\\
(rk-1,r-1)_p^{v-2}=+1,
\end{array}\right.
$$

が得られる。$m=2$ のときも、C_m を適当にとると

$$
(3.6)\quad\left\{\begin{array}{l}
d_1d_2\,rk(rk-2)\sim 1,\\
(d_1d_2,(r-1)^{v-3}(rk-2))_p(-1,d_1d_2)_p(d_1,d_2)_p(-1,r-1)_p^{\frac{v(v-1)}{2}}(-1,rk)_p\\
(v,rk)_p(v,r-1)_p(rk,r-1)_p^{v-1}(-1,r-1)_p^{\frac{(v-2)(v-3)}{2}}(-1,rk-2)_p(v-2,rk-2)_p\\
(v-2,r-1)_p(rk-2,r-1)_p^{v-3}=+1,
\end{array}\right.
$$

ここで

$$\eta_0=\frac{k(k-1)}{v},\quad \eta_1=\frac{(k-1)(rk-1)}{v(r-1)},\quad \alpha=\frac{v-k}{v},\quad \beta=\frac{k}{v}$$

$$\eta_{11}=(k-2)\alpha^2+(v-k)\beta^2,\quad \eta_{12}=-(2k-3)\alpha\beta+(v-2k+1)\beta^2,\quad \eta_{22}=(k-1)\alpha^2+(v-k-1)\beta^2$$

$$\gamma_{11}=[(k-2)\alpha-(v-k)\beta]^2,\quad \gamma_{12}=[(k-2)\alpha-(v-k)\beta][(k-1)\alpha-(v-k-1)\beta]$$

$$\gamma_{22}=[(k-1)\alpha-(v-k-1)\beta]^2$$

$$\rho_{11} = \eta_0 - \frac{\eta_{11}}{r-1} + \frac{\gamma_{11}}{(r-1)(rk-2)}, \quad \rho_{12} = \eta_1 - \frac{\eta_{12}}{r-1} + \frac{\gamma_{12}}{(r-1)(rk-2)},$$

$$\rho_{22} = \eta_0 - \frac{\eta_{22}}{r-1} - \frac{\eta_{22}}{r-1} + \frac{\gamma_{22}}{(r-1)(rk-2)}$$

$$d_1 = \rho_{11}, \quad d_2 = \rho_{22} - \frac{\rho_{12}^2}{\rho_{11}} .$$

これらは、共に identity のようである。$m \geqq 3$ の場合には、C_m の rows と $A_1^{\#}$ の中からうまくとらないと、P が singular になってしまう。

この方法にも、いろいろな変形ができることは明らかであるが、多分すべて identity であると思われる。

4. $\lambda=1$ の場合 (II)

BIBD($\lambda=1$) に付随したいくつかの association schemes が考えられるが、それらが不存在証明に利用できないかという問題がある。

BIBD($\lambda=1$) に付随した association scheme としては、つぎのように各種のものがある。

1°) この BIBD には $\binom{v}{2}$ 個の処理対がすべて1回ずつ配置されているから、$m=b$, $n=\binom{k}{2}$ をパラメターとする GD 型 association が、(同一 block 内の処理対を 1-st associates として) 得られる。

2°) $b \cdot \binom{k}{2}$ 個の処理対に対して、もとの SLB associations で 1-st associates なブロック内の処理対は互に 1-st, 2nd associates なブロック内の処理対は互に 2-nd, 同一ブロック内の処理対は互に 3-rd associates とすると, 3-class association が定義される.

このように, 処理対に関する association や, あるいは $\binom{b}{2}$ 個のブロック対に対する association scheme がいくつか考えられる。

さて, これらの association を利用する一方法として, 任意の処理対 ϕ にある処理対の集合 D_ϕ を対応させ, その正方の結合行列 N の性質を調べることが考えられる。経験的に言えば, このような N は singular な場合が多い。しかがって, Hasse theorem はさもなければ応用できないが, つぎの結果は多少役立つ。

<u>Lemma</u> m-associate class をもつ SPBIBD の結合行列 N のスペクトル分解が

$$NN' = \rho_0 A_0^\# + \sum_{i\in I} \rho_i A_i^\# , \quad (I \subset \mathcal{L}_m = \{1, 2, \cdots, m\})$$

であり, 行列 N が正規 (NN'=N'N) ならば,

(*). $$\prod_{i\in I} \rho_i^{\alpha_i} \sim 1,$$

(**) $$c_p\Big(NN' + \sum_{i\in I^c} A_i^\#\Big) = (-1, -1)_p \quad \text{(すべての素数 } p \text{ について)}$$

が成立する。

時間の余裕があれば, 若干の例を報告する。